UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,310	06/26/2001	Zheng Qi	BRCMP013B	2328

23363 7590 02/15/2006

CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 02/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,310	QI ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3,5-8,11-21,46,48-55 and 68-79* is/are pending in the application.

4a) Of the above claim(s) *1-2, 4, 9-10, 22-45, 47, and 56-67* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3,5-8,11-21,46,48-55 and 68-79* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's arguments/amendments with respect to canceled claim 1-2, 4, 9-10, 22-45, 47, and 56-67, amended claims 3, 5-8, 11-20, 46, 48, 50-51, and 53-55, added claims 68-79, and presently pending claims 3,5-8,11-21,46,48-55 and 68-79, filed on 12/01/2005 have been fully considered but they are moot in view of new ground(s) of rejection.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 11 and 12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Applicant amends claims 11 and 12 wherein "wherein the combined bit sequence is..." It is unclear what applicant wanted to claim because the combined bit sequence does not refer to which combined bit sequence i.e. the first combined bit sequence which is the combination of the first portion of data/first sequence data and the key or the second combined bit sequence which is the combination of the second bit sequence and inverted second bit sequence. Appropriate correction is required in response to this action.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3, 5-8, 11-12, 15, 17-21, 46, 48-49, 51-52, 55, and 68-79 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bruce Schneier (Schneier, Applied Cryptography 1996) in view of Den Boer (Boer, Pub. No: US 20020034295 A1).

Regarding claim 78, Schneier teaches a cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations (page 270 lines 4-24);

an expansion logic expanding a bit sequence associated with a first portion of the data block and generating an expanded bit sequence having a first bit size (page 270 lines 32-33; *the right half of the data is expanded to 48 bits via an expansion permutation logic*);

a first XOR logic performing a first XOR operation of a first key provided by the key scheduler and the expanded bit sequence and generating a first combined bit sequence (page 270 lines 33-34; *XORing the expanded right half of the data with key*);

an Sbox logic taking the first combined bit sequence and generating a second bit sequence having a second bit size smaller than the first bit size (page 270 lines 34; *48 bits expanded data combined with key and sent to S-box and S-box producing 32 new bits*); and

a permutation logic permuting the second combined bit sequence and generating a permuted bit sequence (page 270 lines 35-38; *repeating permutation operation 16 times... for second combined bit sequence...XORed output of function f and left half...*).

Schneier fails to explicitly teach:

an inverse permutation logic performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inversed permutated bit sequence; and

a second XOR logic performing a second XOR operation of the second bit sequence and the inverse permuted bit sequence and generating a second combined bit sequence;

However Boer discloses:

an inverse permutation logic performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inversed permutated bit sequence (par. 38- 0054; *message sub-blocks Mj, j=8-15/second portion are processed by inverse function permutation*);

a second XOR logic performing a second XOR operation of the second bit sequence and the inverse permuted bit sequence and generating a second combined bit sequence (fig. 7 and par. 0054; concatenating/combining/XORing *M0-7 and M8-15 are combined*);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Boer within the system of Schneier because they are analogous in DES cryptography method. One would have been motivated to incorporate the teachings of performing an inverse permutation of the second portioned data and combine the

inverted portion with the second portion to further secure the performance of DES cryptography engine.

Regarding claims 68 and 73, Schneier discloses a cryptography engine/integrated circuit for performing cryptography operations on a data block having a first portion and a second portion, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations (page 270 lines 4-24);

means for combining via a first logical operation a particular key provided by the key scheduler with a first bit sequence associated with the first portion of the data block (page 270 lines 33-34; *XORing the expanded right half of the data with key*);

means for generating a second bit sequence based on the output of the first logical operation (page 270 lines 34; *48 bits expanded data combined with key and sent to S-box and S-box producing 32 new bits*); and

a permutation logic permuting the combined bit sequence and generating a permuted bit sequence (page 270 lines 35-38; *repeating permutation operation 16 times... for second combined bit sequence...XORed output of function f and left half...*).

Schneier fails to explicitly teach:

an inverse permutation logic performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inverse permuted bit sequence; and

means for combining via a second logical operation the second bit sequence with the inverse permuted bit sequence and generating a combined bit sequence;

However Boer discloses:

an inverse permutation logic performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inverse permuted bit sequence (par. 38- 0054; *message sub-blocks Mj, j=8-15/second portion are processed by inverse function permutation*); and

means for combining via a second logical operation the second bit sequence with the inverse permuted bit sequence and generating a combined bit sequence (fig. 7 and par. 0054; concatenating/combining/XORing *M0-7 and M8-15 are combined*);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Boer within the system of Schneier because they are analogous in DES cryptography method. One would have been motivated to incorporate the teachings of performing an inverse permutation of the second portioned data and combine the inverted portion with the second portion to further secure the performance of DES cryptography engine.

As per claims 3, and 46, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the cryptography engine/integrated circuit layout, wherein the cryptography engine is a DES engine (pages 270-285).

As per claim 5, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the cryptography engine, wherein the second bit sequence is less than 32 bits (page 273 last paragraph-275 par. 4; 4-bit... 6-bit...).

As per claims 6, and 48, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the cryptography engine/integrated circuit layout, wherein the first/second bit sequence is four bits (page 273 last paragraph-275 par. 4; 4-bit...).

As per claim 7, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the cryptography engine, wherein the first bit sequence is less than 48 bits (page 273 last paragraph-275 par. 4; 32-bit...4-bit... 6-bit...).

As per claims 8, and 49, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the cryptography engine/integrated circuit layout, wherein the first bit sequence is less than six bits (page 273 last paragraph-275 par. 4; 4-bit...).

As per claim 11 Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the cryptography engine, wherein the combined bit sequence is less than 32 bits (page 270 lines 31-38).

As per claim 12, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the cryptography engine, wherein the combined bit sequence is four bits (page 273 last paragraph-275 par. 4; 4-bit output...).

As per claims 15, and 55, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the cryptography engine/integrated circuit layout, wherein the inverse permutation logic and the permutation logic are associated with DES operations (page 270 lines 4-273; *DES...inverse permutation....expansion permutation*).

Regarding claims 51, and 17-20 Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the integrated circuit layout, wherein the key scheduler comprises a determination stage, a shift stage, a propagation stage, and a consumption stage (page 270 lines 26-274 fig. 12.3).

As per claims 21, and 52, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the cryptography engine/integrated circuit layout, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value (page 271 fig. 12.1).

Regarding claims 69 and 74, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches the cryptography engine, wherein the first and second logical operations are binary XOR operation logic (page 270 lines 26-41).

Regarding claims 70 and 75, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches wherein the first bit sequence is a bit sequence expanded by an expansion logic (page 273 lines 16-35).

Regarding claims 71 and 76, Schneier and Boer teach all the subject matter as described above. In addition, Schneier teaches wherein the second bit sequence is less than the first bit sequence (page 270 lines 34; *48 bits expanded data combined with key and sent to S-box and S-box producing 32 new bits*).

Regarding claims 72, 77, and 79, Schneier and Boer teach all the subject matter as described above. In addition, both teaches wherein the data block contains bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N + 1 to M (Schneier fig. 12.1; *first 32 left half and second 32 right half = 64*, and Boer par. 0038; *M0-7 and M8-15 = M0-15*)

6. Claims 13-14, and 53-54, are rejected under 35 U.S.C. 103(a) as being unpatentable over Bruce Schneier (Schneier, Applied Cryptography 1996) in view of Den Boer (Boer, Pub. No: US 20020034295 A1), and further in view of Steinman et al. (Steinman, U.S. Patent No. 6,591,349 B1).

Regarding claims 13 and 53, Schneier and Boer disclose all the subject matter as described above. Schneier and Boer fail to disclose two-level multiplexer. However Steinman teaches the

cryptography engine/integrated circuit layout, further comprising a multiplexer circuitry including a two-level multiplexer (Steinman Col. 4 lines 1-13).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Steinman with in the combination system of Schneier and Boer because it would allow to increase the performance of computer memory system by reducing lost clock cycles (Steinman Abstract). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to have two 2-to-1 multiplexers on a first level coupled to two 2-to-1 multiplexers on a second level because it would allow to increase the performance of DES or triple DES engine as the performance of the computer improved in using 2-to-1 multiplexers. Speeding up the clock cycle improves the performance of DES.

As per claims 14, and 54, Schneier, Boer and Steinman teach all the subject matter as described above. In addition, the combination teaches the cryptography engine/integrated circuit layout, wherein the multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to an output stage of the multiplexer (Schneier page 270 lines 25-page 272 last paragraph, and Steinman Col. 4 lines 1-13). The rational for combining are the same as claim 13 above.

7. Claims 16, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bruce Schneier (Schneier, Applied Cryptography 1996) in view of Den Boer (Boer, Pub. No: US 20020034295 A1), and further in view of Teppler (U.S. Patent No. 6,792,536 B1).

As per claims 16, and 50, Schneier and Boer teach all the subject matter as described above.

Schneier and Boer do not explicitly teach performing pipelined key scheduling logic.

However Teppler teaches DES pipelining (Teppler Col. 7 lines 13-25)

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Teppler with in the combination system of Schneier and Boer because it would allow to have not impacted system performance (Teppler Col. 7 lines 13-25).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. 5,001,753 *Davio et al. discloses multiple inverse permutation in DES data encryption system for purpose of ensuring security.*

9. Please see Form PTO 892 for more prior art of record.

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.
February 8, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100